Application Delivery Leader

MONITORAPP

AIWSS Service
(Site Checker)

2016

MONITORAPP Co., Ltd.

1. Overview

2. Benefits

3. Features

4. Functions configuration

Services Summary

✔ Site Checker Service

Site Checker Service is a "**Malicious URL Detection Service**" which visits and diagnose the websites regularly to provide proactive defense for the customer's webserver security incident caused by various attacks.

MONITORAPP provides **MUD(Malicious URL Detection)** engine which uses fast website visiting technology to analyze the customer's website.

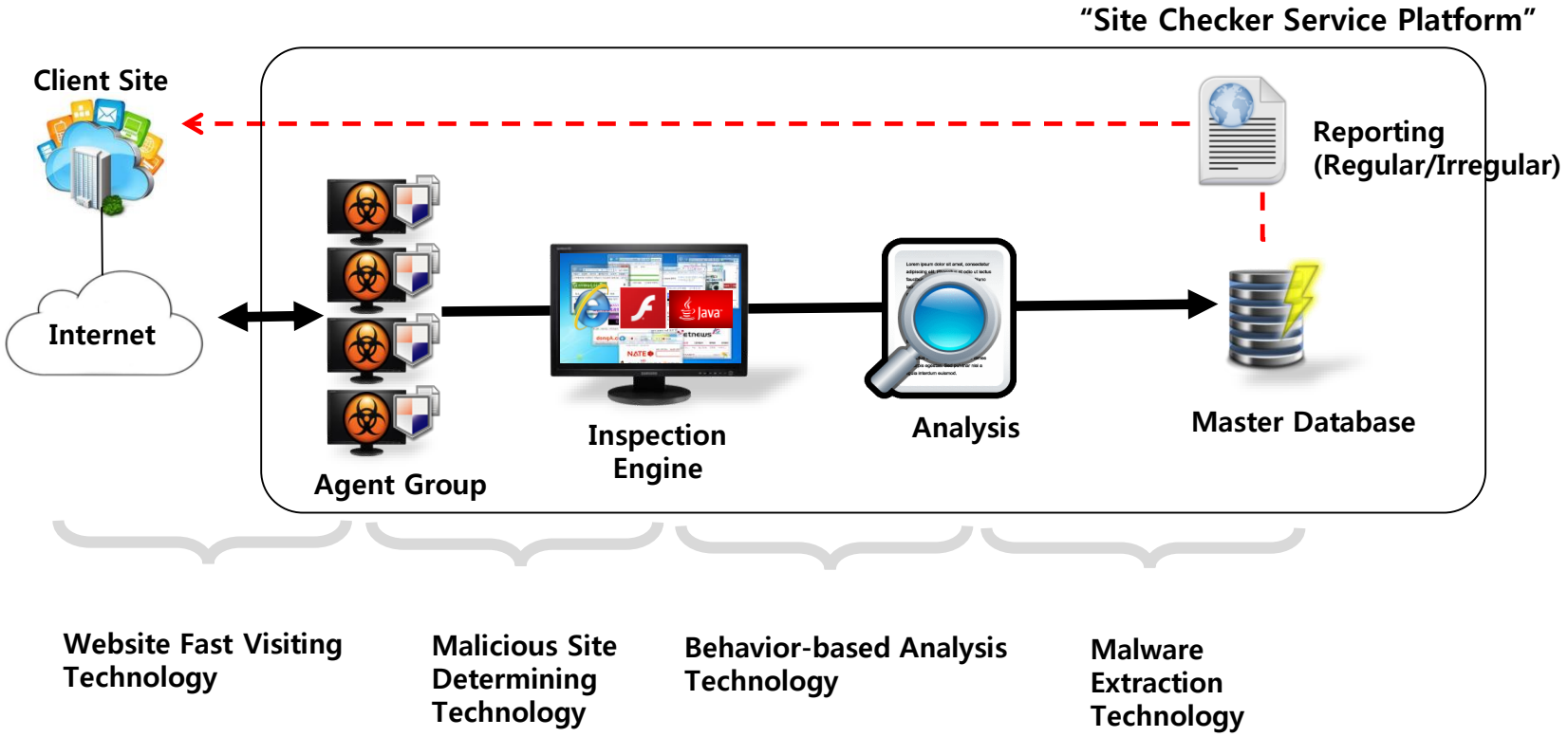
The service determines whether the website is infected by malicious code or is transit/ spreading point of malicious code via behavior-based analysis. It provides proactive defense for the customer's web sever by reporting malicious code-related information (report/ Email/ SMS).

✔ Service Plan

- Service target: the customer's specified websites (including external domain)
- Service delivery method: provides malicious URL/ code detection, analysis, reporting through regular/ irregular fast websites visiting

Services Summary

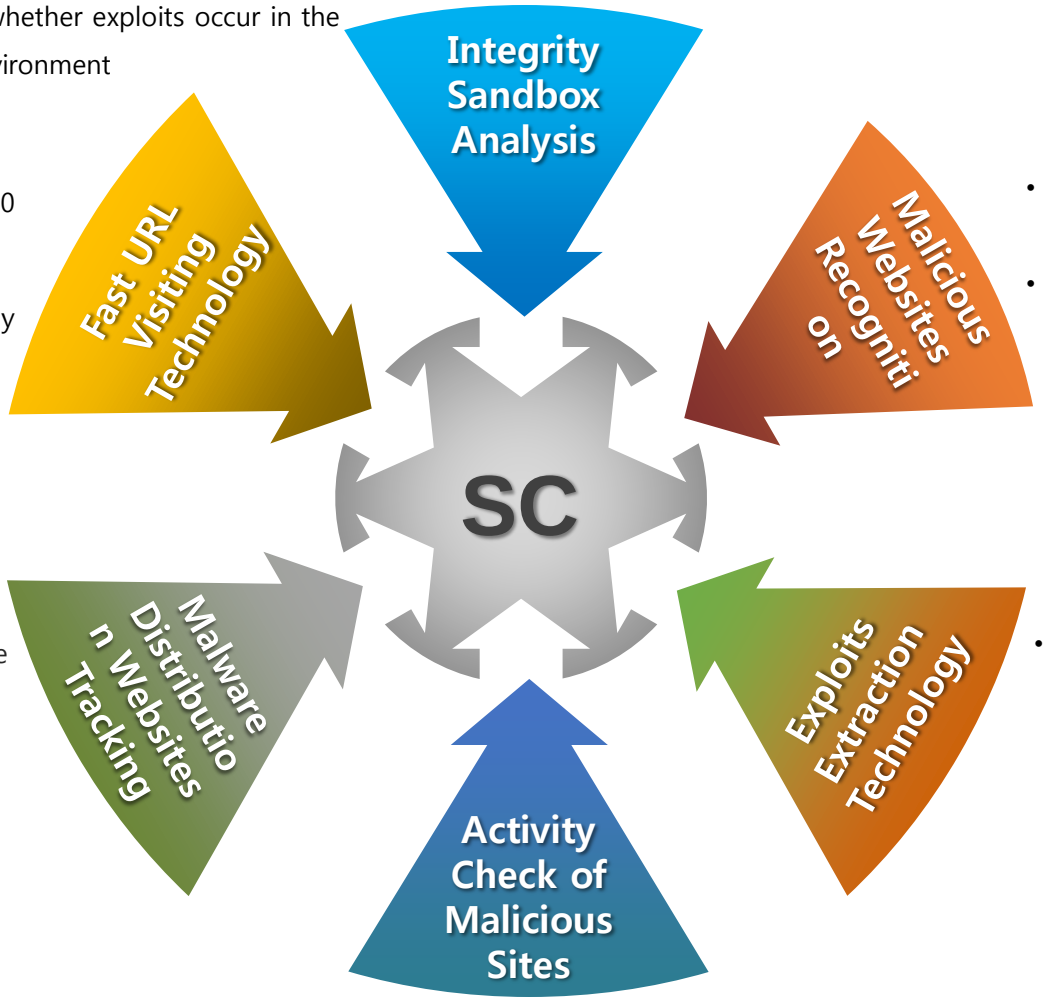
✔ Service Structure



Services Summary

✔ Service Structure

- Determine whether exploits occur in the integrity environment



- Detection of more than 160 malicious URLs monthly
- Sandboxing-based on fast dynamic visiting technology

- Detection whether exploits occurrence is caused by event in the OS
- Behavior-based analysis technology not dependent on patterns

- Tracking of the last website which caused exploits

- Automatic extraction of exploits URL and attack code via multifactor test

Benefits

✔ Website Enhanced Security

After visiting the customer's website via fast visiting technology, diagnostic program determines whether actions that occurs in the OS (processes, registry, file changes, etc.) are exploits through various events detection. Therefore, no mistaken behavior based detection analysis happens and you can protect the web server with trustable information.

✔ Damage Prevention Caused by External Website Infection

On the customer's website connection it is possible to diagnose external website link (selected by user).
Proactive defense against potential additional damage occurring is provided on the customer's website, if the external link is infected by malicious code.

✔ Fast Malicious Code Information Lookup and Analysis Request

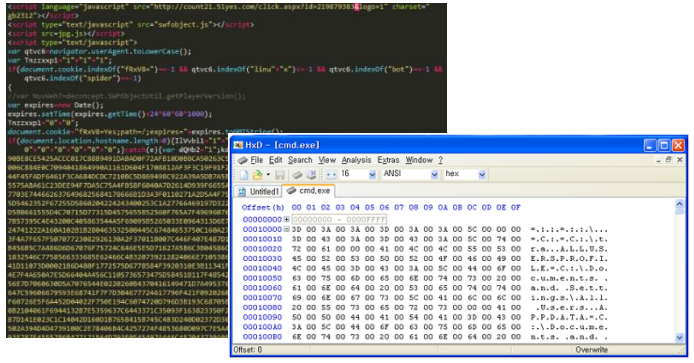
Through the large database of malicious code owned by MONITORAPP, you can check detailed information about malicious code on the website.
For the undefined malicious code, you can request one-click immediate analysis and establish easy preventive measures of malicious code infection.

Sandbox-based Exploit Detection

- Sandbox performs behavior-based analysis directly including encoding and code obfuscation.
- Exploits detection through OS events analysis : insertion process, registry insertion, auto-run files, etc.
- Drive-by-down detection caused by web browsers, plugins, Flash, Java, vulnerability etc.

Application Vulnerability

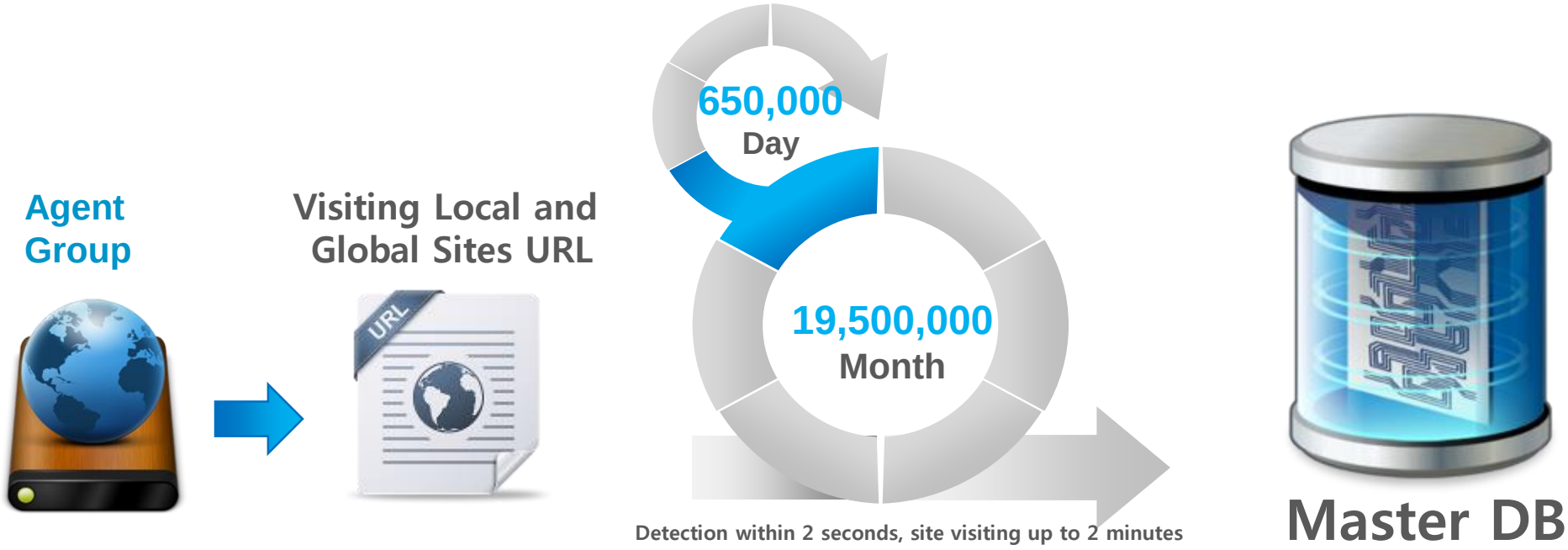
<Application Vulnerabilities>



<Encoding and Obfuscation>

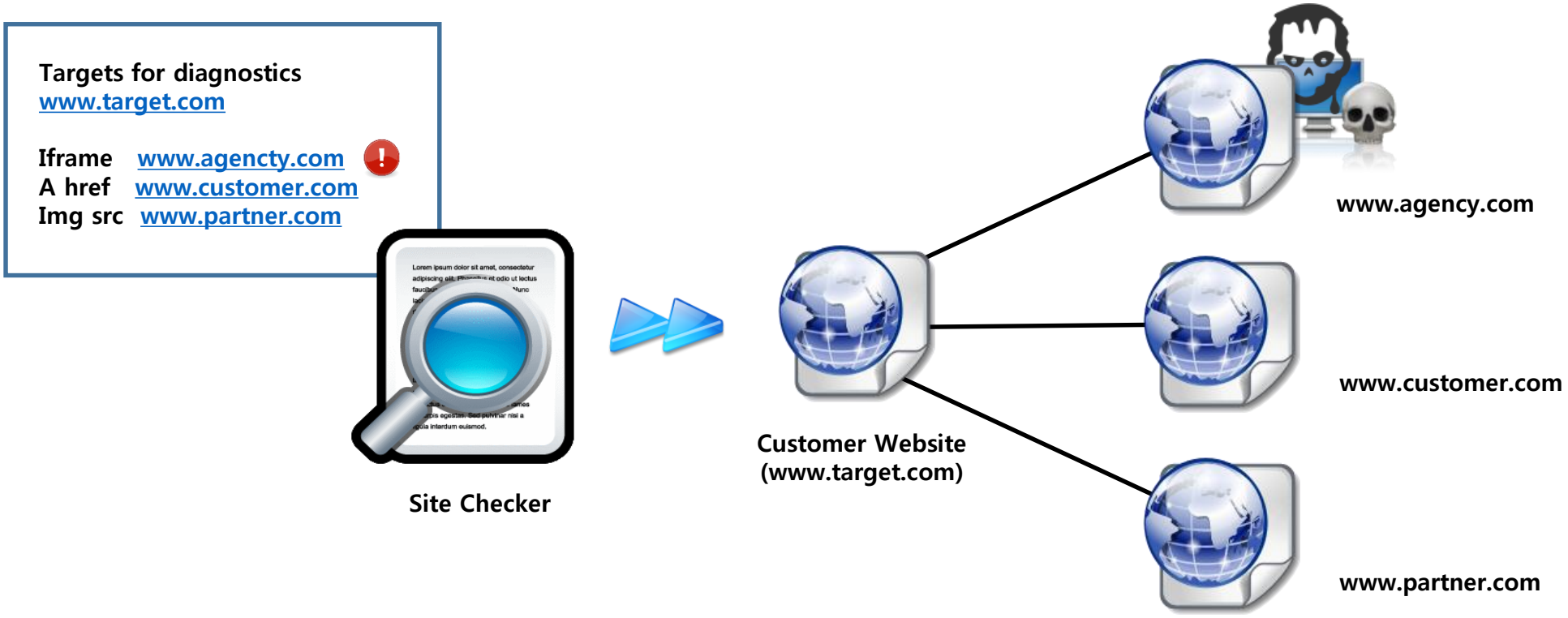
Fast visiting and Large Capacity Malicious Code DB

- Fast visiting MUD(Malicious URL Detection) engine for internal/external websites
- During website verification for infection, connection information for origin expansion, transit and speeding point and malicious code are stored in Master DB.
- It provides detailed information on whether the customer' website is infected with malicious code or provides one-click analysis feature if the malware is undefined.



External Webpage Analysis

- It performs analysis diagnostics of registered website including contained external pages.
- Damage proactive defense through external page infection within the website
- Diagnostics range can be set as follows: all domains/ internal domain/ external domain.



Main Functions

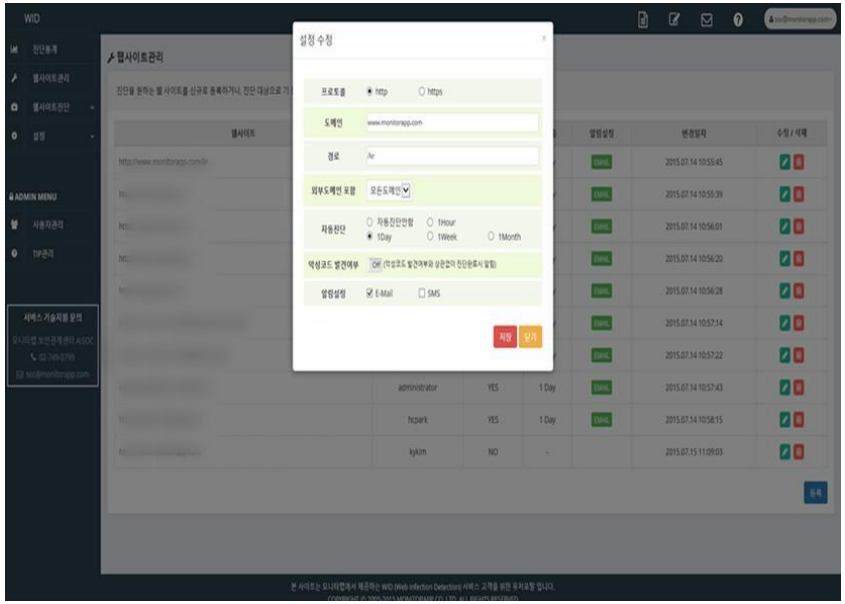
Function	Description
Statistical Information	Provides periodic(day, week, month) diagnostics history and trend statistics
Auto Diagnostic Settings	Websites auto-visiting and analysis on regular basis (by hour, day, week, month)
Real-time Diagnostics Status View	Real-time progress stage checking: website analysis, malicious URL, URL analysis
Malicious Code Details View	Provides information on: malicious code type, location, MD5, malicious code links
Report Auto-Sending on Diagnostics Results	Auto-reporting system on diagnostics history and analysis results
Real-time Notifications on Detection Information	Real-time notification on malicious code detections via Email and/or SMS

Statistical Information

- Provides dedicated “User Interface” for Site Checker
- Provides periodical statistics on malicious code analysis and detection progress

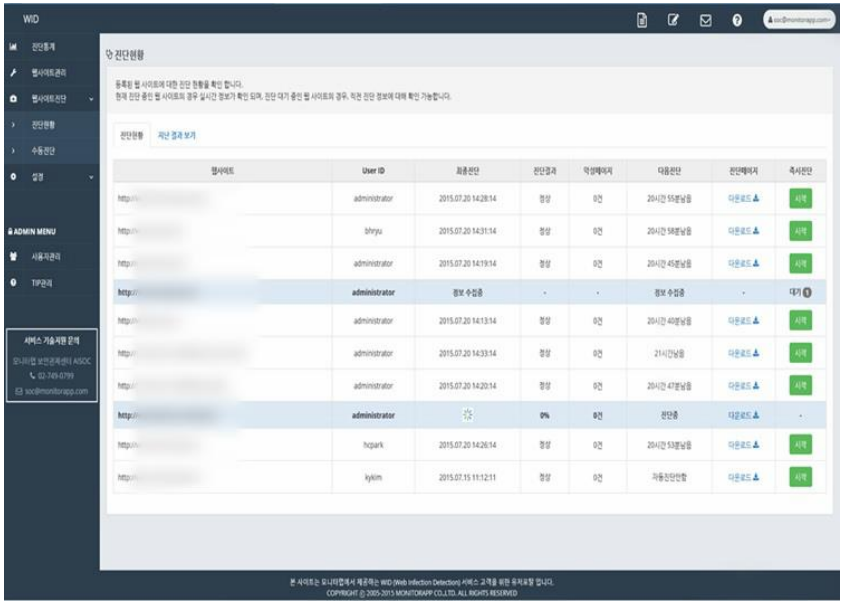
Auto-diagnostic Settings and Status View

✔ Auto Diagnostics Settings



- Performs regular auto-diagnostics and analysis based on website features and priority
- Supports menu for each specific website and diagnosis-related settings

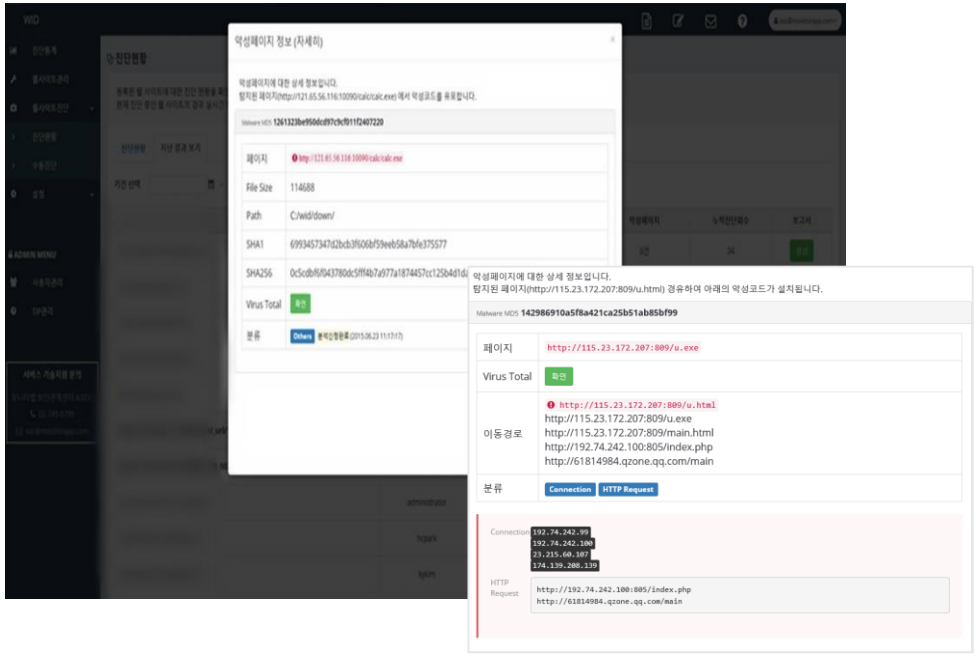
✔ Diagnostic Status View



- Lookups for previous diagnosis history and batch analysis status of entire registered website
- Provides URL list download function of diagnosed target web page

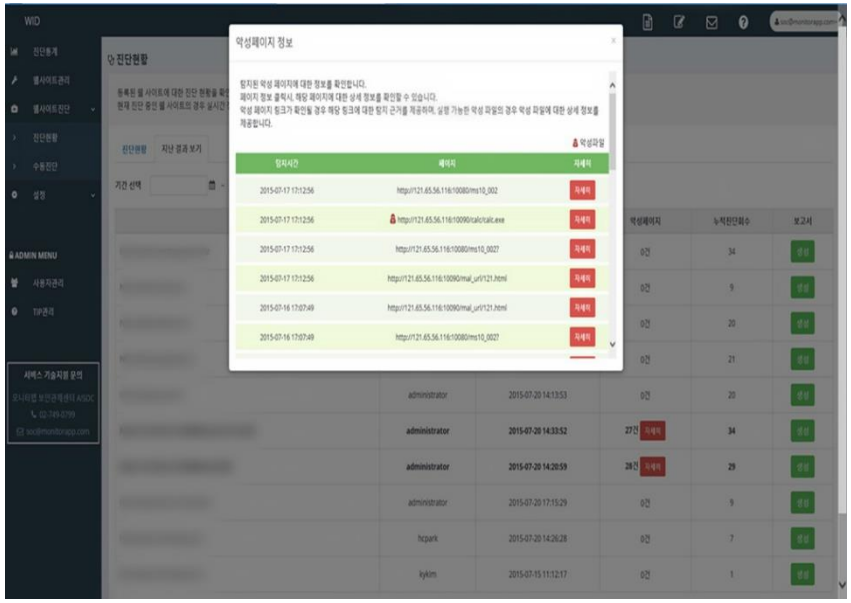
Malicious Code Information Lookup

✔ Malicious Code Information Details



- Provides various malicious code related information detected by sandboxing
- Checks for additional information of malicious code through interwork with Virus Total

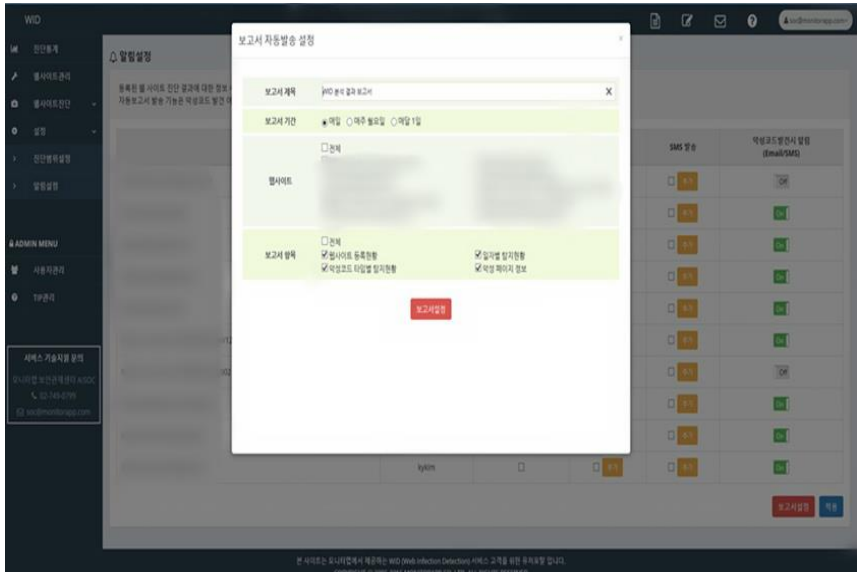
✔ Transit/ Spreading Point Information



- Checks for detection evidence and information of connecting origin expansion, transit and spreading point on infection
- Provides One-click function for requesting malicious code classification analysis

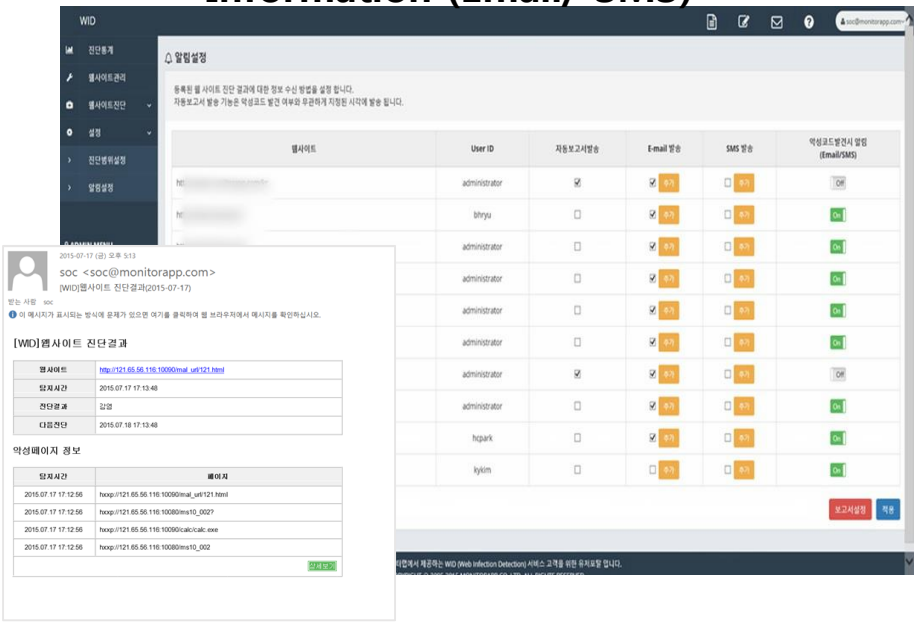
Report of Diagnostics History

✔ Report's Auto-sending Settings



- Ability to send diagnostics history and results
- Reports auto-sending function according to the specified schedule format: daily, weekly, monthly

✔ Real-time Notification on Detection Information (Email/ SMS)



- Real-time notification on malicious detection history by Email/SMS

T H A N K Y O U

MONITORAPP CO., LTD.

306, 38-9, Digital-ro 31-gil, Guro-gu, Seoul, Korea 08376

Tel : +82-2-749-0799, Fax) +82-2-749-0798

E-Mail : soc@monitorapp.com

Website : www.monitorapp.com